Atti del convegno "Intercettazioni, tra esigenze investigative e diritto alla privacy" - 17-18 gennaio 2014

Convegno organizzato a Palermo presso la Sala Magna dello Steri dalla rivista "Sicurezza e Giustizia" e patrocinato dall'associazione ELISS. Sono intervenuti: Giovanni Pitruzzella (Presidente dell'Autorità Garante della concorrenza e del mercato), Sergio Lari (Procuratore della Repubblica di Caltanissetta), Francesca Mazzocco (Sostituto Procuratore di Palermo), Giovanni Di Benedetto (Avvocato del Foro di Palermo), Antonio Scaglione (Ordinario presso Università degli Studi di Palermo), Pasquale Angelosanto (Vice Comandante del Ros carabinieri), Riccardo Lo Verso (giornalista), Francesco Messineo (Procuratore della Repubblica di Palermo), Guido Lo Forte (Procuratore della Repubblica di Messina), Luigi Petrucci (Gip del Tribunale di Palermo), Giuseppe Di Chiara (Ordinario presso Università degli Studi di Palermo), Giovanni Rizzuti (Avvocato del Foro di Palermo), Carlo Marzella (Sostituto Procuratore di Palermo), Andrea Grassi (Vice Direttore dello Sco della Polizia di Stato), Francesco La Licata (giornalista). I giornalisti Riccardo Arena e Lirio Abbate hanno coordinato gli interventi.

Pasquale ANGELOSANTO, laureato in Giurisprudenza e in Scienze della Sicurezza Interna ed Esterna e abilitato all'esercizio della professione forense, è Generale dell'Arma dei Carabinieri e Comandante del Raggruppamento Carabinieri Investigazioni Scientifiche (RACIS). Dal 2009 al 2012 è stato comandante provinciale di Reggio Calabria, ove ha conseguito importanti risultati operativi nel contrasto alla 'ndrangheta e alle sue proiezioni nazionali e internazionali. Dal 2012 al 2014 è stato Vice Comandante del Raggruppamento Operativo Speciale (ROS).

LE INTERCETTAZIONI TELEMATICHE E LE CRITICITÀ DEL *DATA RETENTION* NEL CONTRASTO ALLA CRIMINALITÀ ORGANIZZATA

di Pasquale ANGELOSANTO

1. La minaccia cibernetica[1]. La criminalità organizzata e la telematica

Nel corso di questo mio intervento tratterò argomenti di carattere tecnico-operativo, dall'ottica della polizia giudiziaria, riassunti nel titolo "*Le intercettazioni telematiche e le criticità del data retention nel contrasto alla criminalità organizzata*", partendo dal concetto di minaccia cibernetica[2] che riguarda "*tutte le attività dirette ad accedere, catturare, manipolare o danneggiare l'integrità, la riservatezza, la sicurezza o la disponibilità di dati e informazioni, di un'applicazione o di un sistema senza averne l'autorità*", ovvero come minaccia a "*quello spazio virtuale, che diventa scenario, ove si concretizzano gli interessi oggetto dell'attacco*" (cfr. legge n. 133 del 2012) e, per il tema da affrontare oggi, l'esame sarà circoscritto agli ambiti telematico e delle telecomunicazioni.

Tra le minacce più diffuse posso citare quelle relative alle frodi su Internet e alle richieste estorsive per evitare danni a sistemi informatici o telematici, mentre tra le minacce più pericolose per la collettività e le istituzioni sono da annoverare sicuramente quelle che si caratterizzano in attacchi a infrastrutture sensibili di interesse nazionale o che sfruttano la rete per finalità terroristiche.

A fattor comune, un aspetto caratterizzante le diverse forme in cui si estrinseca la minaccia riguarda la possibilità di effettuare comunicazioni ovunque, con qualsiasi tipo di dispositivo e in maniera sicura; infatti, l'evoluzione della tecnologia delle telecomunicazioni permette oggi a chiunque di potersi connettere alla rete Internet ed utilizzare sistemi telematici per costruire **canali criptati** nei quali veicolare le proprie comunicazioni; il passaggio dai sistemi analogici (i telefoni classici) ai sistemi digitali (comunicazioni cosiddette VoIP[3]) ha garantito la possibilità di utilizzare i sistemi di cifratura e l'affidabilità stessa delle reti telematiche; tali sistemi sono creati e gestiti da società diverse in tutto il mondo, per cui risulta particolarmente difficile decriptare le comunicazioni; un esempio esemplificativo è quello del software Skype, prodotto dall'omonima società prima con sede in Estonia, poi in Lussemburgo e recentemente acquistata da Microsoft, che garantisce la possibilità di comunicazioni audio (VoIP) e video gratuite tra gli utenti registrati e a pagamento (con tariffe

1 Argomenti tratti da uno studio del 2013 del Ten. Col. Luca Flebus, comandante di Sezione del Reparto Indagini Tecniche del ROS.

2 La "cibernetica" come "la scienza legata agli studi dei sistemi di ogni genere che sono in grado di ricevere, immagazzinare e processare informazioni, così da usarle per effettuarne il controllo", secondo la definizione elaborata da Andrej Nikolaevič Kolmogorov (Tambov 25 aprile 1903– Mosca, 20 ottobre 1987), matematico russo. Invece, per "minaccia cibernetica" si intende "l'insieme delle condotte controindicate che possono essere realizzate tramite il cyber-space ovvero in danno di quest'ultimo e dei suoi elementi costitutivi. Si sostanzia in attacchi cibernetici: azioni di singoli individui od organizzazioni (…), finalizzate a distruggere, danneggiare od ostacolare il regolare funzionamento dei sistemi e delle reti (…), ovvero a violare integrità e riservatezza di dati/informazioni. A seconda degli attori e delle finalità, si parla di: a) criminalità cibernetica (cyber-crime): complesso delle attività con finalità criminali (quali, per esempio, la truffa o frode telematica, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali); b) spionaggio cibernetico (cyber-espionage); c) terrorismo cibernetico (cyber-terrorismo)", dal Glossario di Intelligence, edito dalla Presidenza del Consiglio dei Ministri – Sistema di Informazioni per la Sicurezza della Repubblica.

3 In telecomunicazioni e informatica con Voice over IP (Voce tramite protocollo Internet) si intende una tecnologia che rende possibile effettuare una conversazione telefonica sfruttando una connessione Internet o una qualsiasi altra rete dedicata a commutazione di pacchetto che utilizzi il protocollo IP senza connessione per il trasporto dati.

molto basse) verso telefoni fissi e mobili di tutto il mondo; ad oggi il programma Skype è stato registrato da almeno 600 milioni di persone (dati del 2011) ed ha ottenuto un picco massimo di utenti concorrenti di circa 34 milioni nel 2012; si tratta di un fenomeno planetario che consente a chiunque di comunicare in e da ogni parte del globo; i tentativi di monitorare queste comunicazioni da parte della magistratura e degli organismi di polizia giudiziaria hanno sempre trovato complessi ostacoli tecnici.

In egual misura diventano importanti anche altri sistemi di comunicazione, via chat o via VoIP, come Twitter o WhatsApp o Viber o Wechat, tutti facilmente disponibili e scaricabili dalla rete e generalmente ottimizzati per un uso su apparati mobili come gli smartphone, sia nelle piattaforme Android (Samsung ed altri) che IOS (Iphone ed Ipad). Lo scenario che si presenta, almeno per quanto riguarda la parte intercettiva dei canali di comunicazione, è assai complicato, sia per la varietà di sistemi ed applicazioni utilizzate, sia per la possibilità di connettersi praticamente ovunque con linee di collegamento sempre diverse (Wifi aperti, schede UMTS, adsl domestiche, ecc.), con apprezzabili margini di sicurezza per comunicare senza essere individuati e intercettati.

Oggi il contrasto ai fenomeni criminali richiede modalità e procedure sempre più estese e complesse, in quanto la tecnologia ed il suo incessante e rapido sviluppo danno nuove possibilità di comunicazione strumentali alla commissione di delitti.

Due sono i fattori di principale criticità:

(1) delocalizzazione della rete internet: in pratica lo spazio in cui si possono perpetrare i crimini è globale e non ha confini territoriali definiti, in contrasto con le norme di legge che si fondano, viceversa, proprio sul concetto di giurisdizione territoriale. Nello specifico le tecnologie attuali, che prevedono l'utilizzo di risorse distribuite e condivise (c.d. "cloud" – nuvola), ormai superano il concetto di giurisdizione legato al server fisico che custodisce le informazioni di interesse, attualmente utilizzato per la fissazione del luogo del reato;

(2) rapidità di esecuzione e volatilità delle tracce: le attività criminali condotte mediante l'uso di strumenti telematici si realizzano in tempi estremamente concentrati e su più obiettivi contemporaneamente, da sistemi localizzati in siti differenti e distribuiti sull'intera rete mondiale (vedasi attacco mediante reti Botnet – che sta a indicare l'operatività simultanea di migliaia di computer).

In questi settori, inquadrabili nella più ampia minaccia cibernetica, il R.O.S. è stato più volte delegato a svolgere indagini, cercando di fornire di volta in volta soluzioni tecniche in grado di raggiungere il risultato, in quanto l'utilizzo della rete nelle attività delittuose non è certo un problema recente.

Vediamo, allora, alcuni casi concreti, rappresentativi delle più ricorrenti modalità esecutive nella commissione di gravi reati.

1.1 Il sequestro Roveraro

Il 6 luglio del 2006, veniva sequestrato ROVERARO Gianmario[4], che alle ore 01.30 precedenti, dopo aver partecipato ad un incontro conviviale, aveva telefonicamente informato la moglie di trovarsi in Austria con alcune non meglio indicate persone. Nella mattinata del 7 luglio, il predetto richiedeva via fax, alla società YARD di cui era presidente, l'immediata disponibilità della somma di un milione di euro da investire in azioni, avanzando poco dopo la richiesta di un'ulteriore somma di dieci milioni di euro a un consulente finanziario di Lugano, con cui era in affari.
Dalle immediate verifiche tecniche, emergeva che la vittima del sequestro era stato obbligato a effettuare i contatti telefonici utilizzando il sistema SKYPE, rendendo difficilissima l'acquisizione diretta del flusso tramite i gestori di telefonia.
Attraverso una complessa attività di ricerca e la ricostruzione della trasmigrazione dei dati di fonia tra le diverse società interessate allo smistamento del traffico, si riusciva a risalire alla scheda UMTS intestata ad una cittadina ucraina, utilizzata per la connessione SKYPE attraverso un personal computer portatile.
Era così possibile individuare un'altra utenza intestata alla donna, risultata in contatto con ulteriori due utenze aventi numerazione consequenziale.

Le utenze in esame risultavano essersi trasferite da Parma a Milano nel pomeriggio precedente il sequestro, in occasione del quale avevano agganciato proprio la cella ubicata nei pressi dell'abitazione della vittima. In successione, le utenze avevano quindi agganciato i ponti radio della campagna modenese, ove presumibilmente era stato nascosto l'ostaggio. Grazie alle attività di intercettazione e ai contestuali servizi di osservazione e controllo, venivano localizzati e tratti in arresto i sequestratori.

1.2 Il latitante della 'ndrangheta

Nel 2008, nelle indagini per la ricerca e cattura di un pericoloso latitante della 'ndrangheta, capo di una delle più agguerrite cosche della Piana di Gioia Tauro, la preliminare analisi del traffico delle celle, serventi l'area di residenza del ricercato, consentiva di individuare l'esistenza di numerosi collegamenti alla rete internet effettuati tramite sim dati. Si individuava, tra queste, una SIM intestata a un congiunto del latitante che, dopo opportune valutazioni, veniva sottoposta ad intercettazione telematica convenzionale. Gli esiti dell'intercettazione consentivano di riscontrare, nelle diverse fasce orarie, frequenti collegamenti a siti commerciali e pornografici, soprattutto in momenti in cui vi era contezza dai servizi di osservazione che, nell'abitazione monitorata, non doveva esserci la presenza di alcuno. Non potendo avere certezza di chi utilizzasse materialmente il PC, si predisponeva uno studio per un'ulteriore intercettazione telematica che consentiva di catturare il ricercato.

1.3 L'indagine "Tracia"

Nel corso dell'indagine "Tracia" svolta tra il 2002 e il 2004 nei confronti di una organizzazione curda (DHKP-C – "Fronte-Partito Rivoluzionario di Liberazione del Popolo[5]) operante in Turchia veniva dimostrato

4 Nato ad Albenga (SV) il 24.05.1936, residente a Milano in via Alberto da Giussano n° 26, presidente del consiglio di amministrazione della società di investimento YARD con sede a Milano, Piazza Liberty n° 8.

5 Organizzazione terroristica turca di matrice marxista leninista nata nel 1992, che si è resa responsabile in Turchia di numerosi attentati, omicidi di rappresentanti politici e governativi e attentati a obiettivi statunitensi.; in Europa l'attività terroristica era rivolta prevalentemente contro interessi turchi.

che le cellule operative, di cui una attiva anche in Italia, utilizzavano internet per la scambio di file criptati e dissimulati all'interno di file immagini, tramite un sistema steganografico, che permette appunto di nascondervi documenti. Internet era stato utilizzato per la divulgazione delle rivendicazioni degli attentati che venivano inviate dall'Italia a uffici stampa e giornali in Turchia.

La rete è risultata un efficace strumento di comunicazione, reclutamento, finanziamento ed addestramento, sfruttandone, a fini di sicurezza, le potenzialità offerte dal cosiddetto "**web profondo**" (si tratta della rete nascosta, che sfugge ai motori di ricerca ordinari perché i siti non sono indicizzati), ovvero l'utilizzazione di file compressi che sfuggono ai normali motori di ricerca ed il cui accesso è limitato ad utenti in possesso di apposite parole chiave e a conoscenza degli specifici percorsi informatici o addirittura di sistemi di cifratura veri e propri a doppia chiave"[6].

1.4 Gli attentati dei NIPR e NPR (sigle adottate dalle BR-PCC) e l'omicidio Biagi

Il 14 maggio 2000, verso la mezzanotte, in Roma, Via Po n. 16, nei pressi dello stabile dove aveva sede la "COMMISSIONE DI GARANZIA PER L'ATTUAZIONE DELLA LEGGE SULLO SCIOPERO NEI SERVIZI PUBBLICI ESSENZIALI", veniva fatto esplodere un ordigno incendiario collocato su di una bicicletta.

L'attentato veniva rivendicato "tradizionalmente" con un documento cartaceo fatto pervenire presso emittenti radiofoniche e redazioni di quotidiani, a firma del Nucleo di Iniziativa Proletaria Rivoluzionaria, ma la novità investigativa si rilevava il successivo 13 giugno 2000, allorquando la medesima rivendicazione veniva inviata, anche per e-mail, a numerosi indirizzi di posta elettronica, utilizzando un'utenza mobile e un apparato telefonico identificato in un dipositivo Nokia.

Il 10 aprile 2001, alle ore 4.35, deflagrava un ordigno posto all'interno del portone di ingresso dello stabile sito in Roma, via Angelo Brunetti n. 9, sede dell'Associazione per le Relazioni Italia-USA e dell'Istituto Affari Internazionali. L'attentato veniva rivendicato per e-mail (da un account tim.it) con un documento siglato NUCLEO DI INIZIATIVA PROLETARIA RIVOLUZIONARIA, inviato nella mattinata dello stesso giorno.
L'attività d'indagine, sin dalle prime fasi, faceva rilevare nuovamente la particolare caratteristica dell'invio del documento di rivendicazione per posta elettronica (come già avvenuto per l'attentato del 6 luglio 2000 a Milano alla sede della CISL, rivendicato dal Nucleo Proletario Rivoluzionario) e **l'inedito utilizzo** (in Italia e in attentati di matrice eversiva) **di un telefono mobile per l'attivazione di un ordigno esplosivo**. La perizia confermava che all'ordigno utilizzato nell'attentato era stato collegato un apparato telefonico GSM marca Siemens, con funzione di innesco attivato con una chiamata telefonica (impulso).
Il 19 marzo 2002, alle ore 20.10, in Bologna, militanti delle BR-PCC uccidevano a colpi di pistola il Prof. Marco BIAGI. Per l'azione veniva utilizzata la stessa arma che il 20 maggio 1999 era stata utilizzata dalla medesima organizzazione per uccidere il Prof. Massimo D'ANTONA.
Nella serata del 20 marzo 2002 l'azione veniva rivendicata, tramite e-mail (attraverso un account inwind.it), con un documento a firma Brigate Rosse per la costruzione del Partito Comunista Combattente. L'invio della rivendicazione per e-mail (a oltre cinquecento indirizzi di posta elettronica) veniva effettuato lo stesso 20 marzo 2002, tramite telefono cellulare SIEMENS, mentre la casella di posta elettronica risultava essere stata creata pochi minuti prima, presso un Internet Point di Roma.

1.5 L'indagine "Ardire"

Nell'indagine Ardire sviluppata nei confronti di presunti appartenenti alla Federazione Anarchica Informale / Fronte Rivoluzionario Internazionale FAI/FRI, responsabile degli attentati perpetrati nel dicembre 2009[7] e nel dicembre 2011[8], inquadrabili in un rilancio della campagna rivoluzionaria anarchica[9], emergeva che gli anarco-insurrezionalisti avevano una costante necessità di scambiare materiale ideologico a contenuto istigatorio e, soprattutto, di fare da tramite tra le diverse componenti del Fronte Rivoluzionario Internazionale, nonché di coordinare le attività (come le "azioni dirette" violente con l'utilizzo di esplosivi). Ne conseguiva un uso esteso dello strumento telematico, con la inevitabile produzione, nonostante le cautele adottate, di "tracce digitali" che risultavano determinanti ai fini della costruzione dell'impianto accusatorio.

1.6 Alcune attività antagoniste

Il 13 luglio 2013, presso il campeggio NO TAV di Venaus (TO), si è svolto un *meeting* sulla crittografia e sicurezza informatica denominato

6 Parte tratta dall'intervento del Gen. Giampaolo Ganzer, all'epoca Comandante del ROS, al convegno nazionale sul "Terrorismo e contro terrorismo nella cyber war", organizzato dal Centro Studi Difesa e Sicurezza, tenutosi a Roma il 26.02.2008, presso la Camera dei Deputati.

7 Trattasi dei seguenti attentati:

nel tardo pomeriggio del 15 dicembre 2009, presso il "Centro di Identificazione ed Espulsione-CIE" di Gradisca D'Isonzo (GO), deflagrava un plico, pervenuto per posta ed indirizzato al Direttore del Centro. Nel plico veniva rinvenuto un volantino di rivendicazione dal titolo "Operazione Eat The Rich – Fuoco ai CIE ", a firma "Sorelle in Armi/Nucleo Mauricio Morales/FAI";

la notte tra il 15 e il 16 dicembre 2009, presso un tunnel che funge da collegamento fra due strutture dell'Università "Bocconi" di Milano, deflagrava un ordigno artigianale, costituito da un tubo metallico all'interno del quale era stata pressata una consistente quantità di esplosivo. L'azione veniva rivendicata dal "Sorelle in Armi/Nucleo Mauricio Morales/FAI".

8 Trattasi dei seguenti attentati:

il 07 dicembre 2011, a Francoforte (D), presso l'ufficio smistamento posta della Deutsche Bank, perveniva una busta esplosiva, indirizzata all'Amministratore Delegato di quell'istituto; rivendicata dalla "Cellula Free Eat e Billy FAI/FRI";

il 09 dicembre 2011, a Roma, il Direttore Generale di "Equitalia", dr. Marco Cuccagna, rimaneva gravemente ferito a seguito dell'apertura di una busta a lui indirizzata, al cui interno era stato occultato un ordigno. All'interno di una busta di colore giallo, ove era custodita anche la rivendicazione a firma della "Cellula Free Eat e Billy FAI/FRI";

il 12 dicembre 2011, presso l'ambasciata greca di Parigi giungeva una busta con un ordigno esplosivo ove era custodita anche la rivendicazione a firma della "Cellula Free Eat e Billy FAI/FRI".

9 La FAI fa la sua prima apparizione tra il dicembre 2003 ed il gennaio 2004 allorquando, con la Campagna Santa Claus, vengono recapitati alcuni plichi esplosivi ad istituzioni e rappresentanti dell'Unione Europea (tra cui l'allora presidente della Commissione Europea, Romano Prodi). Negli anni successivi al 2004, altre formazioni, anche all'estero, aderiscono al cartello FAI, attraverso numerose iniziative di diversa gravità.

"Crypt'r Die"[10], promosso dagli attivisti legati al gruppo redazionale del noto portale notav.info[11]. L'incontro si proponeva lo scopo di stimolare in Val Susa una "cultura della sicurezza informatica" al fine di sfuggire alle attività repressive delle Forze di polizia.
L'evento si prefiggeva di approfondire le conoscenze:

- sull'impiego massivo del controllo informatico operato mediante monitoraggio delle mailing list e piattaforme di comunicazione (Facebook, Twitter ed altri social network);
- sul controllo psicologico degli individui mediante mail circolanti su siti commerciali;
- sull'uso da parte degli apparati repressivi di applicativi informatici come "*malware*" e virus funzionali a conoscere i contenuti degli hard disk;
- per anonimizzare la navigazione sul web.

2. Le intercettazioni telematiche[12]

In tale quadro, come visto, appare assolutamente indispensabile l'utilizzo di tecniche di intercettazione telematica[13] (captare il flusso telematico di dati, la c.d. on line surveillance) che permettano l'acquisizione di informazioni e contenuti rilevanti in ambito investigativo e quindi probatorio.

Nel tempo, le attività intercettive si sono sviluppate sempre nell'alveo normativo di quanto previsto per le comunicazioni telefoniche, andando a integrarsi nelle previsioni degli articoli del c.p.p.: il 266 per le intercettazioni telefoniche e il 266-bis per quelle telematiche. Tuttavia, questa affinità è venuta presto meno, in quanto le modalità tecniche di attuazione, nel rispetto delle condizioni previste dal codice formale, sono state rapidamente superate dalla tecnologia, che nel campo informatico prima e telematico poi ha sviluppato sempre nuove procedure ed algoritmi (basti pensare che la norma che disciplina le intercettazioni telematiche è stata introdotta con la legge n. 547 del 23.12.1993, di oltre vent'anni fa).

Mettendo da parte le intercettazioni telefoniche (cioè la cattura della fonia), in sostanza, le classiche intercettazioni del traffico dati su linea (telefonica fissa – adsl – e cellulare – umts - definite genericamente "passive") che si basano sulla cattura del traffico duplicato dal provider di telecomunicazioni (gestore), che assicura un servizio di connettività all'indagato, **non forniscono più informazioni e dati di interesse, in quanto la maggior parte del traffico passante risulta cifrato**: in pratica le intercettazioni su linea fissa (ADSL) e mobile (UMTS) permettono solo di accertare che i dispositivi in uso all'indagato sono effettivamente utilizzati, ma non consentono nella stragrande maggioranza dei casi di fornire dati rilevanti, se non i cc.dd "dati esterni", una sorta di tabulato di traffico, molto parziale (traffico verso un determinato sito, senza informazioni di dettaglio sui contenuti dell'esplorazione).

Per questo motivo sono state sviluppate, da parte degli organismi specializzati dei servizi centrali di polizia giudiziaria, con l'ausilio di società di settore, tecnologie in grado di intercettare le informazioni nei punti in cui sono in chiaro, ossia dopo la decodifica direttamente all'interno dei dispositivi.
Tali tecniche vengono generalmente denominate "intercettazioni attive", presupponendo non più solo un ascolto passivo del segnale, ma un'attività di cattura dell'informazione. In sostanza, l'attività di captazione si sposta dalla linea all'interno del dispositivo, trasformandosi da intercettazione in cattura del dato presente nel computer (o nello smartphone), rimanendo nella copertura normativa dell'intercettazione prevista dagli art. 266 e seguenti del c.p.p.

Questi sistemi di decodifica[14] dell'informazione sono estremamente funzionali ma al tempo stesso generano la necessità di essere gestiti in maniera corretta e calibrata sotto i profili investigativo e probatorio; la nuova sfida che ci attende, infatti, sarà quella di essere in grado di operare con strumenti così sofisticati e potenti e riuscire al tempo stesso a garantire, sulla base di quanto previsto dal diritto positivo, la tutela della persona in tutti i suoi ambiti (riservatezza, libertà di comunicazione, inviolabilità del domicilio, ecc.).

In particolare, si possono verificare casi di ambiguità nella fase installativa degli agenti tecnici (captatori informatici); **un esempio è dato dall'intercettazione di un pc pubblico**: in questo caso risulta fondamentale poter intercettare esclusivamente il traffico generato dalla persona indagata e non tutto il traffico generato dal sistema. Un altro caso è quello di un'installazione su un sistema telematico del quale non sia chiara la struttura di rete interna: in questo caso l'individuazione del dispositivo (sistema informatico) da intercettare risulta alquanto difficile e potrebbe accadere che venga monitorato un dispositivo non di interesse investigativo: se ciò accade la polizia giudiziaria deve procedere immediatamente a disinstallare l'agente tecnico laddove si registri una incerta o imperfetta installazione, dandone informazione all'autorità giudiziaria delegante.

Oggi l'uso di tali tecnologie pone necessaria una riflessione su quali siano i riferimenti e gli strumenti normativi da adottare nelle attività operative.

10 Trad. "Crittografa o muori".

11 Cfr. www.notav.info, che riporta le principali notizie della protesta in Val di Susa.

12 Argomenti tratti da uno studio del 2013 del Ten. Col. Andrea Raffaelli, comandante di Sezione del Reparto Indagini Tecniche del ROS.

13 **È necessario chiarire cosa si intende per sistema informatico e invece per sistema telematico, che non sono definiti dalla legge, ma dalla elaborazione giurisprudenziale**. Il sistema informatico, in assenza di una definizione legislativa, è stato definito dalla giurisprudenza come un'apparecchiatura "*destinata a svolgere qualsiasi funzione utile all'uomo attraverso l'utilizzazione, anche solo parziale, di tecnologie informatiche (caratterizzate dalla registrazione, memorizzazione, elaborazione automatica e organizzazione dei dati)*". Più sistemi informatici collegati stabilmente tra loro (via cavo, via radio, wireless, ecc.) per la trasmissione/comunicazione dei dati/informazioni costituiscono un sistema telematico. Tali definizioni hanno poi trovato conforto nell'art. 1 della Convenzione Europea di Budapest del 23 novembre 2001, che ha fornito la definizione di sistema informatico.

14 A tal proposito va specificato che con il termine cattura si definisce generalmente l'attività di raccolta dei dati trasferiti su una rete o passanti attraverso un sistema informatico mentre con quello di decodifica si intende la capacità di un sistema intercettivo di rendere in chiaro il traffico catturato; le intercettazioni passive garantiscono generalmente il 100% del traffico catturato ma solo una piccola parte decodificato (in genere dal 20 al 60 %), mentre quelle attive possono arrivare anche al 100% sia nella cattura che nella decodifica.

Il punto di partenza è costituito dall'art. 266-bis c.p.p., che garantisce in maniera inequivocabile la possibilità di decodificare tutte le informazioni in arrivo ed in partenza da un dispositivo, come ad esempio la navigazione web cifrata e/o le chiamate VoIP anch'esse codificate; allo stesso modo vengono garantite anche le attività di intercettazione cc.dd. "ambientali", disciplinate dall'art. 266 c.p.p.

Maggiore attenzione va invece posta nel caso di attività di ricerca all'interno dei dispositivi, attività che può essere inquadrata nell'ambito della cosiddetta "perquisizione e/o ispezione telematiche[15]", che possono essere eseguite anche "online". In questo caso si tratta del c.d. **monitoraggio** (*on line search* e *one time copy*: ricerca o fotografia istantanea dell'esistente), cioè della captazione del contenuto di un sistema informatico, la c.d. "*perquisizione on line*". Non essendo applicabili le norme che disciplinano le perquisizioni e le ispezioni, che non forniscono una soluzione soddisfacente al caso (la perquisizione è atto a sorpresa, ma garantito), e trattandosi di uno strumento di ricerca della prova non tipizzato, non resta che fare ricorso all'art. 189 del c.p.p , cioè alle prove non disciplinate dalla legge.

L'unica pronuncia della Corte di Cassazione, la sentenza n. 16556 del 29 aprile 2010 (imputato Virruso) fa riferimento a un'indagine del 2004 avente a oggetto un personal computer di un ente pubblico in uso a uno degli indagati. La polizia giudiziaria aveva avviato un monitoraggio occulto e continuativo del sistema informatico, mediante l'uso di un "captatore informatico", pur in assenza di una vera e propria comunicazione con altri utenti (flusso di comunicazioni). La Corte ha ricondotto l'attività al concetto di prova atipica, con conseguente ammissibilità e utilizzabilità. Quindi legittimità del decreto del pubblico ministero nella misura in cui aveva riguardato l'estrapolazione di dati, non aventi a oggetto un flusso di comunicazioni, già formati e contenuti nella memoria del personal computer[16].

Si tratta, come si comprende bene, di attività assolutamente innovative che molto spesso necessitano di una copertura giuridica *ad hoc* e che comunque pongono nuovi orizzonti su cui confrontarsi.
Rimane da un lato sicuramente la necessità di preservare il diritto della privacy di ogni cittadino, ma dall'altro bisogna anche fare una profonda riflessione sul fatto che oggi ogni attività investigativa non può prescindere dall'uso di strumenti di tale portata; le organizzazioni criminali – come detto in apertura - usano i ritrovati della tecnologia per garantirsi impunità e sicurezza nelle comunicazioni. La risposta del Legislatore prima e delle Forze di polizia e della Magistratura dopo dovrà avere la capacità di contrapporre alle diverse forme e all'evoluzione della minaccia efficienti risposte operative, nel rispetto di un quadro normativo aderente alle nuove esigenze investigative e di contrasto.

3. Il Data Retention

Il secondo problema della mia esposizione riguarda la conservazione dei dati generati o memorizzati nella fornitura di servizi di telecomunicazione accessibili al pubblico, per mezzo di reti di comunicazione, relativamente alla durata della loro permanenza nelle memorie dei gestori, che è stata sempre attentamente disciplinata dal Legislatore[17]. La complessità dei dati in questione e il coinvolgimento di milioni di utenti che utilizzano dispositivi portatili rende questo argomento particolarmente delicato, considerando che se da un lato deve essere garantita la riservatezza del singolo cittadino dall'altro vanno rese fruibili le informazioni che possano garantire una accettabile efficacia nelle attività di indagine.

Nell'ambito dei servizi di telefonia mobile la polizia giudiziaria sfrutta da tempo le molteplici informazioni custodite dai gestori. In particolare possiamo distinguere i dati utili, acquisiti dai gestori, nei seguenti:

- traffico fonia, chiamate e messaggistica SMS (permanenza del dato di 24 mesi);
- traffico dati (12 mesi);
- traffico fonia, chiamate non risposte (30 giorni);
- anagrafiche utenti (senza scadenza);
- elenco delle stazioni radiobase (aggiornamenti mensili);
- codici IMEI, circa l'identificazione del modello e tipo di telefono,
- i dati estratti mediante repertamento forense di apparati mobili.

La polizia giudiziaria utilizza tutti i dati elencati per effettuare le necessarie attività di analisi operativa o tattica, impiegando sistemi informativi dedicati, seguendo tradizionalmente due metodi operativi ormai consolidati:

- analisi del traffico telefonico riferito a utenze, allo scopo di ricostruire i legami relazionali fra persone o fra persone e luoghi in un determinato periodo di tempo;
- analisi del traffico telefonico riferito a celle (BTS[18]), finalizzata a evidenziare l'operatività di utenze presenti in determinati luoghi collegati a eventi di interesse investigativo.

Le metodiche appena descritte permettono singolarmente o congiuntamente di offrire oggettivi elementi di riscontro per confermare o escludere ipotesi investigative o stabilire la attendibilità di dichiarazioni testimoniali. In questo contesto operativo, tuttavia,

15 Nel novembre 2001 fu sottoscritta a Budapest la convenzione del Consiglio d'Europa sulla criminalità informatica, recepita in Italia con la legge 18 marzo 2008, n. 48, che ha introdotto rilevanti modifiche nel codice di procedura penale, al Titolo III del Libro III, "Mezzi di ricerca della prova", tra cui in particolare all'art. 244, comma 2, sui casi e forme delle ispezioni, con l'aggiunta di "anche in relazione a sistemi informatici o telematici adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione (art. 8, comma 1, legge 18 marzo 2008, n. 48); all'art. 247, casi e forme delle perquisizioni, con l'introduzione del comma 1-bis, che prevede esplicitamente che "Quando vi è fondato motivo di ritenere che dati, informazioni, programmi informatici o tracce comunque pertinenti al reato si trovino in un sistema informatico o telematico, ancorché protetto da misure di sicurezza, ne è disposta la perquisizione, adottando misure tecniche dirette ad assicurare la conservazione dei dati originali e ad impedirne l'alterazione".

16 Tratto da uno studio del dott. Sergio Colaiocco, Sostituto Procuratore della Procura della Repubblica di Roma, dal titolo "*Nuovi mezzi di ricerca della prova atipici: l'utilizzo dei programmi spia*", pubblicato in Archivio Penale, Fascicolo 1, gennaio-aprile 2014.

17 Articolo 132 del d.lgs. n. 196/2003 del Codice delle Comunicazioni, modificato dal d.lgs. n. 109/2008 (attuazione della direttiva 2006/24/CE riguardante la conservazione dei dati generati o trattati nell'ambito della fornitura di servizi di comunicazione elettronica accessibili al pubblico o di reti pubbliche di comunicazione).

18 Una BTS (Base Tranceiver Station) o SRB (Stazione Radiobase) consiste di un apparato ricetrasmittente dotato di antenne direttive operante su un gruppo di canali radio e diversi da tutte le BTS adiacenti territorialmente, che "serve" un'area geografica opportunamente dimensionata e idonea ad offrire adeguato servizio a tutti gli utenti in essa potenzialmente presenti.

emergono per gli investigatori alcune criticità risolvibili ottimizzando la fornitura obbligatoria di servizi dei gestori ovvero richiedendo la conservazione di ulteriori dati per fronteggiare situazioni operative di emergenza. Vediamo, quindi nel dettaglio alcuni aspetti della tematica, che possono presentare dei margini di miglioramento con minimi investimenti da parte dei gestori, senza che ciò vada a ledere le garanzie di privacy degli utenti.

3.1 Tentativi di chiamata

Negli ultimi anni si è riscontrato un incremento diffuso dell'uso "comunicativo" delle chiamate senza risposta, cioè quelle chiamate originate verso un utente che seppur raggiungibile non risponde alle chiamate ricevute dall'apparato posseduto; in questo caso risulta impossibile ricostruire, oltre i 30 giorni, legami relazionali tra indagati e/o soggetti terzi, ovvero la loro relazione con un evento di interesse investigativo registrato in un determinato momento o luogo. **Sarebbe opportuno, quindi, prolungare la conservazione dei "tentativi di chiamata" da 30 giorni ad un periodo più lungo** (in teoria trattandosi di vera e propria comunicazione non verbale si dovrebbe estendere a 24 mesi come per le chiamate avvenute o rifiutate), specificando anche la durata del tentativo di chiamata (numero degli squilli effettuati). Questa tipologia di contatto telefonico privo di una conversazione assume crescente rilevanza investigativa, costituendo spesso un mezzo di dialogo "codificato" tra gli indagati.

3.2 Blocco di apparati con IMEI alterato o clonato

Il fenomeno consistente nella alterazione del numero IMEI (*international mobile equipment identity*), che caratterizza univocamente ogni singolo apparato di telefonia cellulare, è attualmente molto diffuso. Tale modifica viene effettuata, mediante semplici *software* facilmente reperibili in rete internet, per diversi motivi (consentire l'impiego di un apparato anche con gestori differenti da quello cui originariamente era abbinato, celare l'utilizzo ed evitare il blocco di apparati rubati, permettere l'uso di telefoni importati dall'estremo oriente e non omologati), creando non pochi problemi sul piano investigativo. Tecnicamente l'incremento diffuso di apparati telefonici con numero IMEI identico, perché modificato manualmente per i predetti motivi, crea difficoltà di attribuzione di chiamate all'effettivo apparato che le ha generate e confusione nella localizzazione di un utente all'interno di una cella radiobase, se sono presenti altri apparati con medesimo IMEI. Inoltre, cosa più grave, sono già stati segnalati casi anomali di captazione di conversazioni avvenute fra utenti estranei alle indagini che dispongono di un apparato con IMEI identico ad un altro IMEI inserito come target di intercettazione autorizzata.

3.3 Conservazione dei dati contenuti nel database VLR delle reti cellulari

Ciascun gestore, all'interno della propria rete cellulare, dispone di diversi *database* che, abbinati a porzioni di territorio più o meno ampie, mantengono memorizzate alcune informazioni relative agli utenti in quel momento presenti nella loro area di competenza. Fra queste informazioni, sempre aggiornate, ci sono quelle che devono consentire la localizzazione dell'utenza nel momento in cui è necessario instradarle una chiamata entrante. Tuttavia se il telefono viene spento alcuni dati di localizzazione rimangono in memoria per poco tempo (qualche ora) e vengono cancellati anche perché allo stato non fanno parte delle forniture di servizio obbligatorie.
Per scopi di sola localizzazione sarebbe opportuno che i gestori conservassero per un periodo di tempo adeguato i dati temporaneamente memorizzati nei *database* denominati VLR (*Visitor Location Register*), per sfruttare alcuni importanti dati tra i quali quelli di localizzazione di utenti che in quel momento sono presenti nel territorio di pertinenza (per esempio, basti pensare ai soli vantaggi che ne deriverebbero nelle attività di ricerca delle persone scomparse).

4. Conclusioni

Alla luce di quanto evidenziato diventa indispensabile **adeguare gli strumenti normativi alle mutate esigenze operative**, auspicando che il nostro Legislatore fornisca alla polizia giudiziaria e alla magistratura requirente mezzi più aderenti a un più efficace contrasto alle azioni della criminalità organizzata, mafiosa e terroristica, che come abbiamo visto è pronta a sfruttare rapidamente tutte le innovazioni tecnologiche che vengono introdotte sul mercato.
Inoltre, è opportuno proporre, in ambito internazionale, le seguenti iniziative finalizzate ad un'attività di contrasto più efficace e aderente ad uno scenario in continuo cambiamento. In particolare, appare necessario:

- garantire una cooperazione più stretta in ambito internazionale, valutando l'opportunità di utilizzare al meglio gli organismi internazionali di polizia (come Europol) e della Autorità Giudiziaria (come Eurojust) al fine di ottenere un raccordo normativo unico soprattutto in merito alle questioni inerenti la tipologia dei reati e dei diritti di privacy (ad esempio, ci si può riferire ai differenti tempi di data retention dei tabulati telefonici);
- rendere tempestivo e velocizzare il più possibile lo scambio informativo relativo ai modelli di comportamento criminale (modus operandi) e le tecniche impiegate per attuare le minacce, facendo uso di strumenti telematici adeguatamente dimensionati e sicuri (trattandosi di sistemi di controllo, questi devono essere gestiti da organi in grado di impiegarli secondo affidabili procedure autorizzative e di tutelare la riservatezza dei dati acquisiti) gestiti dagli attuali organi comunitari preposti e accessibili ai soggetti legittimati al contrasto (Forze di polizia, Magistratura, Organismi di Sicurezza).

Del resto, la stessa Convenzione di Budapest del 23 novembre 2001, ratificata con la legge n. 48 del 2008, all'art. 23, già fissava i principi generali relativi alla cooperazione internazionale stabilendo che "*Le parti devono cooperare tra loro nella misura più ampia possibile nelle indagini o nei procedimenti riguardanti i reati collegati a sistemi e dati informatici, o per raccogliere le prove, in forma elettronica, di un reato, in conformità alle disposizioni di questo capitolo e in applicazione degli strumenti internazionali sulla cooperazione internazionale in materia penale, degli accordi stipulati sulla base di una legislazione uniforme o in condizione di reciprocità e del loro diritto nazionale*". ©